NATIONAL WEATHER SERVICE INSTRUCTION 60-704
November 14, 2003

Information Technology
IT Security

Technical Controls

NOTICE: This publication is available at: http://www.nws.noaa.gov/directives/.

OPR: W. Martin **Certified by:** B. West
Type of Issuance: Initial

SUMMARY OF REVISIONS:

Signed by Barry C. West 10/31/03
Barry C. West Date
Chief Information Officer

Table of Contents

1 Introduction. Technical controls focus on security controls that the computer system executes. These controls provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. System owners will employ technical controls consistent with the requirements of Federal Regulations, DOC and NOAA policies, procedures, and guidelines to ensure adequate protection of all IT resources. Controls applied will consist of:

Identification and Authentication
Logical Access Controls
Warning Banners
Audit Trails

2 Definitions.

2.1 Classified and Unclassified Systems. A system is considered "classified" if it is used, to electronically process, store, or transmit classified data. IT security requirements apply equally to classified and unclassified systems, but the rigor with which controls are implemented is greater for classified systems commensurate with the higher risk associated with classified data.

2.2 General Support System. According to National Institute of Standards and Technology Special Publication 800-18, a General Support System is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and

people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

2.3 Major Application. According to National Institute of Standards and Technology Special Publication 800-18, a Major Application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

3 Identification and Authentication. Identification and authentication controls are a technical measure that prevent unauthorized people (or unauthorized processes) from entering or executing an IT system. The user identification tells the system who the user is. The authentication mechanism provides an added level of assurance that the user really is who they say they are. Authentication consists of something a user knows (such as a password), something the user has (such as a token or smart card), or something the user is (such as a fingerprint). All NWS IT systems will have a means to enforce user accountability for their use of the system, so that system activity (both authorized and unauthorized) can be traced to a specific user. The implementation or technology used should provide access security commensurate with the level of sensitivity assigned to the resource (i.e. information, devices or systems). All DOC IT systems and associated equipment that rely on passwords as the means to authenticate users must implement effective password management in accordance with the DOC Policy on Password Management.

3.1 Maintenance of User ID's. All user ID's for NWS IT Systems will belong to currently authorized users. Identification data will be kept current by adding new users and deleting former users. Deactivation of all computer system accounts must occur within 24 hours of notification to the system administrator of a change in user status when the account user:

departs the agency voluntarily or involuntarily;
transfers to another operating unit within the agency;
is suspended;
goes on long term detail; or
otherwise no longer has a legitimate business need for system access.

This action will occur in a timely manner consistent with the circumstances of the user's change in status, but under no condition, longer than the next day. User ID's that are inactive on a system for 45 days must be removed. The status of an account will be checked at 15 and 30 days and removed at 45 days, if the account does not become active.

3.2 Password Management. The term password in this section refers to passwords, access control codes and password lists. Any compromise of passwords through any means described herein will be reported using the NOAA Incident Response Procedures on the NOAA Security Web site at https://www.csp.noaa.gov. Passwords assigned to individual users will be the primary means used to authenticate a user's access to IT resources (computer systems and networks). Passwords are the first technical line of defense against unauthorized access. All NWS IT System passwords will conform to the DOC Password Management Policy requirements

3.2.1 Passwords will be at least eight characters in length;

3.2.2 Passwords must be composed of representatives of at least two of the following character sets: upper case and lower case English; numeric characters; 6 non-repeating characters; and, special characters. It is strongly recommended that representatives from all three of the character sets be used. NOAA provides information on how to construct user passwords in the NOAA Computer users guide at https://www.csp.noaa.gov/usersguide/index.html .

3.2.3 All passwords will have a maximum password lifetime of 90 days. Systems will have an automated mechanism to ensure that users change their passwords at an interval not greater than 90 days.

3.2.4 User accounts will be suspended after three invalid password attempts. Legacy systems without this capability will ensure manual procedures are in place to limit the life cycle of passwords to 90 days.

3.2.5 NWS IT system and network resources will maintain a queue of previously used passwords. For each user, the password queue will store a minimum of the user's eight most recent passwords and be protected against re-use by the user.

3.3 Password Policy Waiver. The NWS Chief Information Officer is required to identify any deviation from the mandatory practices of this policy and must request a waiver in writing from the DOC IT Security Manager. Approved waivers must be documented as part of the appropriate system security plan(s) that cover the system(s) applicable to the waiver. Identical systems under the same management authority and covered by one system security plan require only one waiver request. Requests for a password management waiver must include:

3.3.1 The specific mandatory practice(s) for which the waiver is requested

3.3.2 The rationale for the requested waiver

3.3.3 If applicable, describe compensating controls to be in place during the period of the requested waiver, and until systems are made compliant with this policy

3.3.4 A Plan of Action and Milestone (POAM) which outlines actions to be initiated to bring the system into compliance with DOC policy

3.4 Use of Passwords to Protect Data. In addition to system level passwords, NWS IT Systems will use algorithmic and view-based access controls implemented by operating systems, security subsystems, or database management systems (e.g., file attributes, access control lists, security rules, object-oriented security labels, database sub-schemas) to control access to sensitive data. All IT passwords stored on a device for authentication will be encrypted using an approved encryption method (e.g., Triple-DES, AES, etc). Operating system provided encryption is considered acceptable. Passwords will not be displayed on the monitor.

3.5 Initial Password. An initial password is one defined by a manufacturer, system administrator or computer systems security officer and given to a user to enable access. FIPS 112, section 3.5, Ownership, requires that "personal passwords used to authenticate identity will be owned (i.e., known) only by the individual who created the private data." Therefore, new NWS IT Systems will have the ability to allow new users to change their passwords after initial access to a system. Where applicable, systems will be configured to require the user to select a new password after signing on with an initial password. Any operating system or applications system "feature" that would allow a system administrator to view passwords will be disabled. All system default passwords, including service accounts, will be changed as soon as possible after system installation and before becoming operational.

3.6 Password Distribution. FIPS 112, section 3.6, Distribution, requires that "Personal passwords will be distributed from the password source in a way that only the intended owner may see or obtain the password." Initial passwords will be created and distributed by local system administrators/security administrators that have direct contact with system users. Transport of passwords for purposes of issue or reference lists to perform maintenance functions will be controlled.

3.7 Password Control Procedures. Passwords will never be stored in open text files for any reason on IT resources. This includes wireless devices, fixed and mobile computers, portable media, or other IT subject to theft or loss. Passwords will not be openly stored on web sites. Once passwords are issued, they are the responsibility of the user and will be protected from inadvertent compromise. Inadvertent compromise results from poor or careless control practices. System owners will establish procedures to ensure distributed or transported passwords are controlled and traceable to the person issued. Such procedures could include; the use of mail and tracking logs (sealed envelope), use of the telephone is allowed if a call is made to the new user's authorized work phone number and an effort is made to verify the user's identity based upon a personal identifier, voice recognition, information on an access request form, etc. (the user will immediately log on and change his or her password). The use of portable media (floppy disks or compact disks) with encrypted or password protected files issued one time to individuals responsible for maintaining multiple systems is acceptable for transporting or distributing lists or multiple passwords.

3.8 One-Time Password or Token. One-time passwords are those that have a limited lifetime, i.e. a few minutes or less. Use of token assisted authentication will be strongly considered in new systems for users having an extraordinary level of access to system resources. This category includes system and security administrators. One-time passwords may be randomly generated or selected by the system administrator and delivered to the user.

3.9 Use of Cryptography for User Authentication. The use of Cryptography or Cryptographic Exchange that meets the Federal Information Processing Standard (FIPS) Publication 140-1, Security Requirements for Cryptographic Modules, may be used instead of passwords to authenticate user access to systems.

4 Logical Access Controls (Authorization/Access Controls). Logical access controls are the system-based mechanisms used to specify who or what (e.g., in the case of a process) is to have access to a specific system resource and the type of access that is permitted. Where appropriate, NWS IT Systems will employ the controls necessary to authorize or restrict the activities of users and system personnel within the system. Where practical hardware or software features designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists) will be used. All access controls will follow the concept of "least privilege" which requires that a user be given no more privilege than necessary to perform a job. All access (physical and electronic) to NWS IT Systems is restricted to trusted employees, contractors, and vendors. NWS Network/System Administrators (N/SA) and IT System Security Officers (ISSO) will develop individual policies that define the authority that will be granted to each user, or class of users of non-programmatic resources. System plans and procedures will describe any restrictions to prevent users from unauthorized access to the system or applications outside of normal work hours. The following are specific logical access controls to be applied or considered for all NWS IT Systems.

4.1 Roles or Position Based Controls. All NWS UNIX workstations provide Discretionary Access Controls (DAC) using standard UNIX mode permission bits which limit and control access to system resources and prevent deliberate or accidental corruption of critical data files. These controls will be applied wherever practical.

4.2 Access Control Lists (ACLs). Systems will have an ACL, or register of the users and types of access allowed. If DACs or ACLs are not used, processes or procedures will be implemented to restrict users from accessing operating systems or sensitive software configurations.

4.3 Screen Blanking. All NWS computers must be configured to conceal the desktop display after no more than 15 minutes inactivity, using a password protected mechanism.

4.4 Sensitive File Access. Encryption will be used to prevent unauthorized access to sensitive files as part of the system or application access control procedures.

4.5 Remote Access. Remote access to NWS resources will be granted on a case-by-case basis and only with prior approval of management or security official. Failure to obtain approval for remote access will be considered a breech of security.

4.6 Internet Access. Internet access for operational resources is limited to that described by programmatic policy or procedure. Internet access for administrative systems is limited to established local access policy plans and procedures. Uncontrolled, unauthorized (e.g., viewing of sexually explicit material, engaging in prohibited discriminatory conduct, etc.) access to the internet by any user with operational resources will be considered a violation of the DOC, NOAA and NWS IT security policies.

4.7 Wide Area Networks. Wide Area Network connectivity will be limited to DOC, NOAA, and NWS approved access methods and system requirements. Uncontrolled, unauthorized connection to the internet or any other Wide Area Network(s) by any user will be considered a violation of the DOC, NOAA and NWS IT security policies.

4.8 Perimeter Protection. A network boundary is the point at which your network attaches to other networks or devices not under your control or to the Internet. Various devices reside near the perimeter of your network, most critical among them, the perimeter security /border devices (border routers) and firewalls, which provide direct external connections. Because boundary connections are so vital and vulnerable, NWS must have procedures and definitions in place to describe their network perimeter. System owners must ensure that configurations for perimeter security device management (e.g., Telnet, secure shell) allow communication between only those IP addresses that are explicitly set in the configuration. Perimeter security devices will be configured to maintain a separate access password that conforms to the DOC Policy on Password Management.

5 Hardware and Software Controls. Hardware and software controls are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. The process of configuration management provides for a controlled environment in which changes to hardware and software are properly authorized, tested, and approved before implementation. System owners must establish procedures for configuration management of all general support systems and major applications. The system security plan must describe how changes to the system or application will be authorized, controlled, tested, and implemented.

5.1 Configuration of Communications Ports (software and hardware). In order to maintain network security, the security staff must monitor all of the entry points into the network. An unauthorized, and therefore unknown and unattended, entry point can result in a serious security breach. All unused ports must be disabled to prevent access to the system.

5.2 Use of Security Labels. Security lables will be used to control access to sensitive information or files and lables will specify protective measures or indicate additional handling instructions.

5.3 Malicious Software. When malicious software is detected by either a user or an administrator the incident must be report in accordiance with NOAA Incident response reporting procedures on the NOAA Security Web site at https://www.csp.noaa.gov

5.3.1 Virus Protection. A Virus is infectious or invasive software that attacks a computer system. The software can either be benign and simply be a nuisance, and it can be destructive to the system. All viruses are a reportable security incident. Virus protection software is required, and the system N/SA or ITSSO will provide users with installation, training and support. Anti-Virus software for all NWS IT Systems is provided via NOAA Security Office. The NOAA provided **a**nti-virus is required on all computer resources that connect to the network directly or via remote access services.

6 Warning Banners. Public Law 99-474 requires that a warning message be displayed, notifying unauthorized users that they have accessed a U.S. Government computer system and unauthorized use can be punished by fines or imprisonment. All NWS IT resources capable of being accessed by communication connections, and providing interactive "login" services will display a warning message at the time of login. The warning message will be displayed prior to asking for any user identification and is the first message from the IT system that the user sees. The word "Welcome" will never appear as part of the "login" process. The NWS ITSO will maintain the lastest version of accepted screen login warning banners for IT resources as described or distributed by NOAA. Warning banners will be used on all interactive logins to NWS equipment in accordance with Federal Regulations, DOC and NOAA policy. Legacy major systems not able to support warning banners will have plans to support this capability in the next major upgrade. The NWS ITSO will maintain a set of the current approved warning banners. The choice of which screen warning banner to implement is the system owners and will be based on system-specific technology limitations, data sensitivity, or other unique system requirements.

7 Audit Trails. Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. Audit trails will be employed on all serving systems or devices and critical operational resources. For administrative use only, workstation auditing will be as required by the system owner. NWS serving systems will generate chronological logs of all system activity. The information is available for review by N/SA's and will be saved to off-line archives and be available for review by the ISSO and NWS ITSO upon request. System security related logs will be retained for a minimum of 30-days. Backups of logs will be made in order to assure their integrity before they are finally archived. Summaries of computer system activity and operations logs will be reviewed on a daily basis. The N/SA and assigned ITSSO for systems will ensure procedures detect departure from established procedure and policy for the following

7.1 Attempted and Successful remote logins

7.2 Telnet and File Transfer Protocol (FTP) events
7.3 RPC port calls
7.4 Data handling into and out of systems
7.5 Message Handling System (MHS) activities